(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 113628049 A
(43)申请公布日 2021.11.09

(21)申请号 202110823741.X

(22)申请日 2021.07.21

(71)申请人 三峡大学
地址 443002 湖北省宜昌市西陵区大学路8号

(72)发明人 蔡政英 董子昱 张起源 黄悦华 张磊

(74)专利代理机构 宜昌市三峡专利事务所 42103
代理人 余山

(51)Int.Cl.
G06Q 40/04(2012.01)

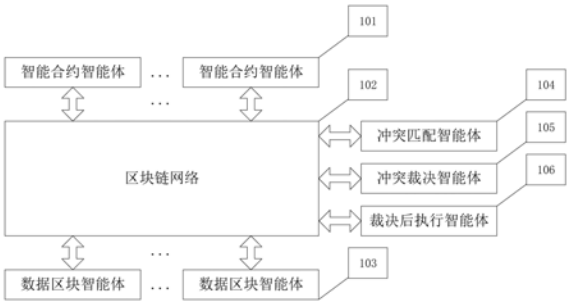
权利要求书4页 说明书13页 附图2页

(54)发明名称

一种基于群体智能的区块链智能合约的冲突裁决方法

(57)摘要

一种基于群体智能的区块链智能合约的冲突裁决方法,包括以下步骤:步骤1,裁决初始化;步骤2,冲突匹配;步骤3,冲突裁决;步骤4,裁决执行;在步骤1中,设置冲突裁决参数,多个智能合约智能体采集智能合约和交易消息,通过区块链网络将智能合约参数和交易消息输入冲突匹配智能体;在步骤2中,多个冲突匹配智能体根据智能合约智能体发送来的智能合约参数和交易消息,通过区块链网络检索数据区块智能体,进行冲突匹配,将冲突匹配结果送入冲突裁决智能体;本发明的目的是为了解决区块链智能合约中交易冲突的判断和裁决问题,通过群体智能方法实现交易冲突的快速判断和交易冲突的智能裁决,提高智能合约运行的效率和区块链工作的安全性。



CN 113628049 A

1.一种基于群体智能的区块链智能合约的冲突裁决方法,其特征在于,包括以下步骤:

步骤1,裁决初始化;

步骤2,冲突匹配;

步骤3,冲突裁决;

步骤4,裁决执行;

在步骤1中,设置冲突裁决参数,多个智能合约智能体(101)采集智能合约和交易消息,通过区块链网络(102)将智能合约参数和交易消息输入冲突匹配智能体(104);

在步骤2中,多个冲突匹配智能体(104)根据智能合约智能体(101)发送来的智能合约参数和交易消息,通过区块链网络(102)检索数据区块智能体(103),进行冲突匹配,将冲突匹配结果送入冲突裁决智能体(105);

在步骤3中,多个冲突裁决智能体(105)根据冲突匹配智能体(104)发送来的冲突匹配结果进行冲突裁决,并通过区块链网络(102)将冲突裁决结果发送到裁决后执行智能体(106);

在步骤4中,多个裁决后执行智能体(106)根据冲突裁决智能体(105)发送来的裁决结果,通过区块链网络(102)控制智能合约智能体(101)和数据区块智能体(103)的执行。

2.根据权利要求1所述的方法,其特征在于,所述步骤1,具体包括以下步骤:

子步骤1-1,设置冲突裁决参数;设置冲突裁决使用的相关参数,包括冲突匹配智能体(104)的数量,订单编码,时间戳或时间属性,区块链的长度,区块链的分支数,地理位置或空间属性,买家确认情况,卖家确认情况,算力值和占比,进一步地,不同智能合约设置不同类型码、智能合约编码、订单编码、匹配属性参数,有效匹配阈值;还包括冲突裁决智能体(105)的数量,时间属性,空间属性,裁决的准则,裁决的主要步骤和对应参数;还包括裁决后执行智能体(106)的数量,属性,执行的主要步骤和对应参数;

子步骤1-2,采集智能合约参数;通过多个智能合约智能体(101)采集本次交易使用的智能合约,并分析智能合约使用的参数,包括智能合约类型码、智能合约编码、合约订单编码,智能合约的属性,智能合约执行的主要步骤,主要步骤的参数,智能合约签名方法,加密方式;

子步骤1-3,采集交易消息;通过多个智能合约智能体(101)采集本次交易的信息,并分析交易参数,包括交易对象属性,交易对象单价,交易数量,交易金额,交易时间,交易单编号,交易方信息,支付信息,关联银行信息;

子步骤1-4,信息发送;通过区块链网络(102)将冲突裁决参数发送给冲突匹配智能体(104),冲突裁决智能体(105),裁决后执行智能体(106),并将采集的智能合约参数和交易消息发送给冲突匹配智能体(104)。

3.根据权利要求1所述的方法,其特征在于,所述步骤2,具体包括以下步骤:

子步骤2-1,智能体接收消息;多个冲突匹配智能体(104)接收智能合约智能体(101)发送来的智能合约参数和交易消息;多个冲突匹配智能体(104)对智能合约参数和交易消息进行预处理和分类,并打上智能合约类型码;

子步骤2-2,冲突匹配;多个冲突匹配智能体(104)通过区块链网络(102)检索数据区块智能体(103),进行冲突匹配;多个冲突匹配智能体(104)检查智能合约类型码与数据区块智能体(103)中智能合约类型码相匹配的频率和不匹配的频率,由子步骤1-1中设置的有效

匹配阈值判断是否发生冲突;若匹配的频率高于设置的有效匹配阈值,则判定为无冲突,可继续执行智能合约完成交易;若匹配的频率低于设置的有效匹配阈值,则判定为有冲突,需要进行冲突裁决,方可完成交易;

子步骤2-3,属性匹配值计算;属性匹配值用于度量智能合约冲突匹配的差异程度,包括智能合约参数和交易信息的不同属性的相异之处,全部属性匹配值用于冲突裁决时参考;可用于冲突匹配的属性,包括订单编码,时间戳或时间属性,区块链的长度,区块链的分支数,地理位置或空间属性,买家确认情况,卖家确认情况,算力值和占比,进一步地,不同智能合约设置不同匹配属性参数;若不同属性匹配的差值低于设置的有效匹配阈值,则属性匹配值越低;若不同属性匹配的差值高于设置的有效匹配阈值,则属性匹配值越高;进一步地,根据智能合约参数和交易信息计算出全部的时间属性、空间属性、智能合约匹配属性参数的属性匹配值;

子步骤2-4,匹配值输出;计算出的智能合约类型码匹配频率和多个属性匹配值共同作为本次冲突的匹配值,并由多个冲突匹配智能体(104)将冲突匹配值送入冲突裁决智能体(105)。

4.根据权利要求1所述的方法,其特征在于,所述步骤3,具体包括以下步骤:

子步骤3-1,冲突匹配值输入;

子步骤3-2,群体智能裁决计算;多个冲突裁决智能体(105)对冲突匹配结果进行冲突裁决计算,更新交易冲突在智能合约交易中的空间位置;按照式(2)调整合约冲突智能体在智能合约编码向量空间的移动速度以及方向,再根据式(3)对合约冲突智能体的智能合约编码向量空间位置进行更新;

子步骤3-3,群体智能优化裁决结果;优选地,使用粒子群-遗传混合算法产生的最优裁决结果对冲突智能体进行全局搜索;粒子群-遗传混合算法在整个智能合约冲突空间中寻找最优的裁决结果,其初始种群大小对应智能合约冲突数量,适应度值对应冲突匹配值;粒子位置对应冲突向量编号,即空间位置属性;粒子的速度对应向量变化的速度,即合约冲突的时间属性;遗传算法中选择、交叉、变异算子对应冲突向量的选择、向量的交叉和向量的变异;

子步骤3-4,裁决结果输出;得到最优的冲突裁决结果后,可以由多个冲突裁决智能体(105)通过区块链网络(102)将冲突裁决结果发送到裁决后执行智能体(106)。

5.根据权利要求4所述的方法,其特征在于,在步骤3-1中,具体包括以下步骤:

步骤1)多个冲突裁决智能体(105)接收冲突匹配智能体(104)发送来的冲突匹配值;优选地,冲突裁决智能体(105)使用粒子群-遗传混合算法;

步骤2)假设产生n个交易冲突,初始化智能合约类型码匹配频率Q_{min}和Q_{max},冲突裁决算法交叉概率process,冲突裁决算法迭代次数N_iter,交易冲突的数据范围bound,匹配的频率阈值r^0,冲突裁决使用的遗传算法进化代数maxgen,匹配属性匹配值阈值A^0,遗传算法种群规模sizepop,遗传算法变异概率pmutation;

步骤3)在对应的智能合约编码向量空间内,设第i个合约冲突智能体的智能合约编码向量空间位置为X_i,$i\in(1,2,\cdots,n)$,针对不同属性计算与之对应的匹配值Fitness(Xi);

步骤4)计算全局最优匹配值f_{min}、对应的最优冲突向量x^*;

$$Q_i=Q_{min}+(Q_{max}-Q_{min})\times rand \qquad (1)$$

$V_i^t = V_i^{t-1} + (V_i^t - X^*) \times Q_i$ (2)

$X_i^t = X_i^{t-1} + V_i^t$ (3)

$X_{new}(i) = X^* + 0.01 \times randn(1,d)$ (4)

其中：、X_i^t、X_i^{t-1}为合约冲突智能体i分别处于t次迭代及t-1次迭代情况下的智能合约编码向量空间位置，即空间属性；V_i^t、V_i^{t-1}为合约冲突智能体i分别处于t次迭代及t-1次迭代情况下的向量飞行速度，即时间属性；X^*表示当前全局最优位置；Q_i表示合约冲突智能体i对区块链智能合约的交易条件进行搜索时的智能合约类型码匹配值，即类属性匹配值；$Q_{min} \leqslant Q_i \leqslant Q_{max}$；randn为产生均值为0，方差$\sigma^2=1$，标准差$\sigma=1$的正态分布的随机变量，d为合约冲突向量的维数。

6.根据权利要求4所述的方法，其特征在于，在步骤3-2中，具体包括以下步骤：

步骤1)随机产生一个随机数rand1；若$rand1 > r^0$，则：通过式(4)生成与之对应的最优合约冲突智能体，作为备选裁决结果，然后完成局部搜索；

步骤2)计算出冲突匹配值，也就是fitba，该值即为备选最优位置对应的冲突匹配值；

步骤3)为了减少算法的时间复杂度，增加算法的通用性、匹配性和健壮性，本算法通过离差的方法选取与全局最优值差异最小的冲突智能体后代作为最优子代并计算冲突匹配值，记为fitgaba；

步骤4)比较fitba和fitgaba，最小值记为F_{new}；选择冲突匹配值较小的个体作为局部搜索后的交易冲突向量的位置，并记录为冲突裁决结果；进一步地，测量不同智能合约的不同匹配属性参数，包括订单编码，时间戳或时间属性，区块链的长度，区块链的分支数，地理位置或空间属性，买家确认情况，卖家确认情况，算力值和占比，依次计算这些属性的匹配值；

步骤5)为了减少局部扰动对裁决结果的影响，优选地，统计100次以上迭代的结果，进一步地，统计区块链智能合约中的交易冲突中智能合约类型码相匹配的频率和不匹配的频率；进一步地，选用更多的迭代次数能够更好地降低局部扰动对频率统计和裁决结果的影响。

7.根据权利要求4所述的方法，其特征在于，在步骤3-3中，具体包括以下步骤：

步骤1)随机生成rand2，如果$rand2 < A^0$，匹配属性匹配值阈值A^0，对比当前智能合约的交易冲突向量的位置和匹配值是否产生变化，如果有所变化，就将其移动到与之对应的更新处；否则，不更新位置信息；

步骤2)计算裁决优化目标函数；针对现在交易冲突向量的空间位置属性匹配值F_{new}和全局最优属性匹配值f_{min}进行比较；若是$F_{new} <= f_{min}$，则将全局最优位置属性值X^*、局部最优冲突匹配值f_{min}一起进行更新；进一步地，根据不同智能合约的不同匹配属性参数进行裁决优化，用户可以根据不同智能合约的特点选择不同的属性作为裁决优化目标函数，包括订单编码，时间戳或时间属性，区块链的长度，区块链的分支数，地理位置或空间属性，买家确认情况，卖家确认情况，算力值和占比，并计算所选择的所有属性的最优裁决方案；进一步地，裁决方案的评估是多目标的，裁决的优化目标可以考虑区块链的分叉最少，或单根区块链的长度最长，交易时间间隔最小，算力约束小于51％；

步骤3)计算最近两次裁决优化结果的精度误差有没有小于ε_1，或进行裁决优化是否达到最大次数限制；如果误差符合精度要求或达到最大次数限制，则进行下一个子步骤，输出裁决结果；如果误差不符合精度要求或未达到最大次数限制，则返回到前一子步骤，继续优

化裁决结果。

8.根据权利要求4所述的方法，其特征在于，在步骤3-4中，具体包括以下步骤：

步骤1)根据群体智能算法输出的最优裁决向量的位置，判断冲突匹配值大小，对交易冲突裁决结果按匹配值高低进行排序，以便于后续的冲突执行按照优化的冲突匹配值从高到低处理；进一步地，可以根据用户需求对冲突裁决结果按交易优先级排序，以便于后续的冲突执行按照优先级从高到低处理；

步骤2)把最优交易冲突向量的位置、与之相应的冲突匹配值、属性匹配值、排序结果输出。

9.根据权利要求1所述的方法，其特征在于，所述步骤4，具体包括以下步骤：

子步骤4-1，接受裁决结果；多个裁决后执行智能体(106)接收冲突裁决智能体(105)发送来的裁决结果，包括对应的智能合约、冲突匹配值、属性匹配值；

子步骤4-2，智能合约智能体执行；对应的智能合约执行裁决结果，由多个裁决后执行智能体(106)通过区块链网络(102)控制智能合约智能体(101)的执行；

子步骤4-3，数据区块智能体执行；多个裁决后执行智能体(106)通过区块链网络(102)控制数据区块智能体(103)的执行；

子步骤4-4，执行结果返回；返回本次记账结果，以及区块链的长度。

10.一种基于群体智能的区块链智能合约的冲突裁决系统，其特征在于，它包括多个智能合约智能体(101)、区块链网络(102)、多个数据区块智能体(103)、多个冲突匹配智能体(104)、多个冲突裁决智能体(105)、以及多个裁决后执行智能体(106)；多个智能合约智能体(101)与区块链网络(102)双向连接，多个数据区块智能体(103)与区块链网络(102)双向连接，多个冲突匹配智能体(104)与区块链网络(102)双向连接，多个冲突裁决智能体(105)与区块链网络(102)双向连接，多个裁决后执行智能体(106)与区块链网络(102)双向连接。

一种基于群体智能的区块链智能合约的冲突裁决方法

技术领域

[0001] 本发明属于区块链技术领域，具体涉及一种基于群体智能的区块链智能合约的冲突裁决方法。

背景技术

[0002] 区块链网络是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用 模式。智能合约基于区块链，在区块链上运行，智能合约是一种旨在以信息化方式传播、验证或 执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且 不可逆转。只有当某一事件触发后，智能合约才会立即执行，这样用计算机语言取代法律语言来 记录条款的合约用数学和编程的形式定义了一系列合约双方的权利和义务，一旦被特定的交易触 发，就可被自动执行。基于区块链系统的智能合约不仅具有其本身所具备的成本效率等优势，还 可避免恶意行为对其正常执行的干扰，有着自动化，去中心化，结果确定的特性，一旦被部署在 区块链上，就不会停止，这也保障了其在存储、读取、执行等过程公正透明、记录可追踪、不可 被篡改。

[0003] 但是，在区块链智能合约中还存在冲突问题，如何在智能合约交易进行有效的冲突裁决是提 升区块链系统安全性的关键问题。但是，现有的区块链技术和智能合约在尚未有有效机制进行冲 突裁决，从而制约了区块链智能合约交易的推广应用。目前，市场上也未有一种基于群体智能的 区块链智能合约的冲突裁决方法。

[0004]

发明内容

[0005] 本发明的目的是为了解决区块链智能合约中交易冲突的判断和裁决问题，通过群体智能方法 实现交易冲突的快速判断和交易冲突的智能裁决，提高智能合约运行的效率和区块链工作的安全 性。

[0006] 一种基于群体智能的区块链智能合约的冲突裁决方法，包括以下步骤：

[0007] 步骤1，裁决初始化；设置冲突裁决参数，多个智能合约智能体采集智能合约和交易消息， 通过区块链网络将智能合约参数和交易消息输入冲突匹配智能体；主要子步骤包括：子步骤1-1， 设置冲突裁决参数；子步骤1-2，采集智能合约参数；子步骤1-3，采集交易消息；子步骤1-4， 信息发送；

[0008] 步骤2，冲突匹配；多个冲突匹配智能体根据智能合约智能体发送来的智能合约参数和交易 消息，通过区块链网络检索数据区块智能体，进行冲突匹配，将冲突匹配结果送入冲突裁决智能 体；主要子步骤包括：子步骤2-1，智能体接收消息；子步骤2-2，冲突匹配；子步骤2-3，属性 匹配值计算；子步骤2-4，匹配值输出；

[0009] 步骤3，冲突裁决；多个冲突裁决智能体根据冲突匹配智能体发送来的冲突匹配结果进行冲 突裁决，并通过区块链网络将冲突裁决结果发送到裁决后执行智能体；主要子步骤包括：子步骤 3-1，冲突匹配值输入；子步骤3-2，群体智能裁决计算；子步骤3-3，群体智

能优化裁决结果；子步骤3-4，裁决结果输出；

[0010] 步骤4，裁决执行；多个裁决后执行智能体根据冲突裁决智能体发送来的裁决结果，通过区 块链网络控制智能合约智能体和数据区块智能体的执行；主要子步骤包括：子步骤4-1，接受裁 决结果；子步骤4-2，智能合约智能体执行；子步骤4-3，数据区块智能体执行；子步骤4-4，执 行结果返回。

[0011] 所述的方法，其特征在于，所述步骤1，冲突信息采集，包括以下步骤：

[0012] 子步骤1-1，设置冲突裁决参数；设置冲突裁决使用的相关参数，包括冲突匹配智能体的数 量，订单编码，时间戳或时间属性，区块链的长度，区块链的分支数，地理位置或空间属性，买 家确认情况，卖家确认情况，算力值和占比，进一步地，不同智能合约设置不同类型码、智能合 约编码、订单编码、匹配属性参数，有效匹配阈值；还包括冲突裁决智能体的数量，时间属性， 空间属性，裁决的准则，裁决的主要步骤和对应参数；还包括裁决后执行智能体的数量，属性， 执行的主要步骤和对应参数；

[0013] 子步骤1-2，采集智能合约参数；通过多个智能合约智能体采集本次交易使用的智能合约， 并分析智能合约使用的参数，包括智能合约类型码、智能合约编码、合约订单编码，智能合约的 属性，智能合约执行的主要步骤，主要步骤的参数，智能合约签名方法，加密方式；

[0014] 子步骤1-3，采集交易消息；通过多个智能合约智能体采集本次交易的信息，并分析交易参 数，包括交易对象属性，交易对象单价，交易数量，交易金额，交易时间，交易单编号，交易方 信息，支付信息，关联银行信息；

[0015] 子步骤1-4，信息发送；通过区块链网络将冲突裁决参数发送给冲突匹配智能体，冲突裁决 智能体，裁决后执行智能体，并将采集的智能合约参数和交易消息发送给冲突匹配智能体；

[0016] 所述的方法，其特征在于，所述步骤2，冲突匹配，包括以下步骤：

[0017] 子步骤2-1，智能体接收消息；多个冲突匹配智能体接收智能合约智能体发送来的智能合约 参数和交易消息；多个冲突匹配智能体对智能合约参数和交易消息进行预处理和分类，并打上智 能合约类型码；

[0018] 子步骤2-2，冲突匹配；多个冲突匹配智能体通过区块链网络检索数据区块智能体，进行冲 突匹配；多个冲突匹配智能体检查智能合约类型码与数据区块智能体中智能合约类型码相匹配的 频率和不匹配的频率，由子步骤1-1中设置的有效匹配阈值判断是否发生冲突；若匹配的频率高 于设置的有效匹配阈值，则判定为无冲突，可继续执行智能合约完成交易；若匹配的频率低于设 置的有效匹配阈值，则判定为有冲突，需要进行冲突裁决，方可完成交易；

[0019] 子步骤2-3，属性匹配值计算；属性匹配值用于度量智能合约冲突匹配的差异程度，包括智 能合约参数和交易信息的不同属性的相异之处，全部属性匹配值用于冲突裁决时参考；可用于冲 突匹配的属性，包括订单编码，时间戳或时间属性，区块链的长度，区块链的分支数，地理位置 或空间属性，买家确认情况，卖家确认情况，算力值和占比，进一步地，不同智能合约设置不同 匹配属性参数；若不同属性匹配的差值低于设置的有效匹配阈值，则属性匹配值越低；若不同属 性匹配的差值高于设置的有效匹配阈值，则属性匹配值越高；进一步地，根据智能合约参数和交 易信息计算出全部的时间属性、空间属性、智能合

约匹配属性参数的属性匹配值；

[0020] 子步骤2-4，匹配值输出；计算出的智能合约类型码匹配频率和多个属性匹配值共同作为本 次冲突的匹配值，并由多个冲突匹配智能体将冲突匹配值送入冲突裁决智能体；

[0021] 所述的方法，其特征在于，所述步骤3，冲突裁决，包括以下步骤：

[0022] 子步骤3-1，冲突匹配值输入；

[0023] 子步骤3-1a，多个冲突裁决智能体接收冲突匹配智能体发送来的冲突匹配值；优选地，冲突 裁决智能体使用粒子群-遗传混合算法；

[0024] 子步骤3-1b，假设产生n个交易冲突，初始化智能合约类型码匹配频率Q_{min}和Q_{max}，冲突 裁决算法交叉概率process，冲突裁决算法迭代次数N_iter，交易冲突的数据范围bound，匹配的 频率阈值r^0，冲突裁决使用的遗传算法进化代数maxgen，匹配属性匹配值阈值A^0，遗传算法种群 规模sizepop，遗传算法变异概率pmutation；

[0025] 子步骤3-1c，在对应的智能合约编码向量空间内，设第i个合约冲突智能体的智能合约编码 向量空间位置为X_i，i∈(1，2，…，n)，针对不同属性计算与之对应的匹配值Fitness(Xi)；

[0026] 子步骤3-1d，计算全局最优匹配值f_{min}、对应的最优冲突向量X^*；

[0027] $Q_i=Q_{min}+(Q_{max}-Q_{min})\times rand$ (1)

[0028] $$V_i^t = V_i^{t-1} + (V_i^t - X^*) \times Q_i \quad (2)$$

[0029] $$X_i^t = X_i^{t-1} + V_i^t \quad (3)$$

[0030] $X_{new}(i)=X^*+0.01\times randn(1,d)$ (4)

[0031] 其中：、X_i^t、X_i^{t-1}为合约冲突智能体i分别处于t次迭代及t-1次迭代情况下的智能合约编码向 量空间位置，即空间属性；V_i^t、V_i^{t-1}为合约冲突智能体i分别处于t次迭代及t-1次迭代情况下 的向量飞行速度，即时间属性；X^*表示当前全局最优位置；Q_i表示合约冲突智能体i对区块链智 能合约的交易条件进行搜索时的智能合约类型码匹配值，即类属性匹配值；$Q_{min}\leqslant Q_i\leqslant Q_{max}$；randn为产生均值为0，方差$\sigma^2=1$，标准差$\sigma=1$的正态分布的随机变量，d为合约冲突向量的 维数；

[0032] 子步骤3-2，群体智能裁决计算；多个冲突裁决智能体对冲突匹配结果进行冲突裁决计算， 更新交易冲突在智能合约交易中的空间位置；按照式(2)调整合约冲突智能体在智能合约编码向 量空间的移动速度以及方向，再根据式(3)对合约冲突智能体的智能合约编码向量空间位置进行 更新；

[0033] 子步骤3-2a，随机产生一个随机数rand1；若rand1>r^0，则：通过式(4)生成与之对应的最 优合约冲突智能体，作为备选裁决结果，然后完成局部搜索；

[0034] 子步骤3-2b，计算出冲突匹配值，也就是fitba，该值即为备选最优位置对应的冲突匹配值；

[0035] 子步骤3-2c，为了减少算法的时间复杂度，增加算法的通用性、匹配性和健壮性，本算法通 过离差的方法选取与全局最优值差异最小的冲突智能体后代作为最优子代并计算冲突匹配值，记 为fitgaba；

[0036] 子步骤3-2d，比较fitba和fitgaba，最小值记为F_{new}；选择冲突匹配值较小的个体作为局部 搜索后的交易冲突向量的位置，并记录为冲突裁决结果；进一步地，测量不同智

能合约的不同匹 配属性参数,包括订单编码,时间戳或时间属性,区块链的长度,区块链的分支数,地理位置或 空间属性,买家确认情况,卖家确认情况,算力值和占比,依次计算这些属性的匹配值;

[0037] 子步骤3-2e,为了减少局部扰动对裁决结果的影响,优选地,统计100次以上迭代的结果, 进一步地,统计区块链智能合约中的交易冲突中智能合约类型码相匹配的频率和不匹配的频率; 进一步地,选用更多的迭代次数能够更好地降低局部扰动对频率统计和裁决结果的影响;

[0038] 子步骤3-3,群体智能优化裁决结果;优选地,使用粒子群-遗传混合算法产生的最优裁决结 果对冲突智能体进行全局搜索;粒子群-遗传混合算法在整个智能合约冲突空间中寻找最优的裁 决结果,其初始种群大小对应智能合约冲突数量,适应度值对应冲突匹配值;粒子位置对应冲突 向量编号,即空间位置属性;粒子的速度对应向量变化的速度,即合约冲突的时间属性;遗传算 法中选择、交叉、变异算子对应冲突向量的选择、向量的交叉和向量的变异;

[0039] 子步骤3-3a:随机生成rand2,如果rand2＜A^0,匹配属性匹配值阈值A^0,对比当前智能合 约的交易冲突向量的位置和匹配值是否产生变化,如果有所变化,就将其移动到与之对应的更新 处;否则,不更新位置信息;

[0040] 子步骤3-3b:计算裁决优化目标函数;针对现在交易冲突向量的空间位置属性匹配值F_{new}和 全局最优属性匹配值f_{min}进行比较;若是F_{new}＜＝f_{min},则将全局最优位置属性值X^*、局部最优 冲突匹配值f_{min}一起进行更新;进一步地,根据不同智能合约的不同匹配属性参数进行裁决优化, 用户可以根据不同智能合约的特点选择不同的属性作为裁决优化目标函数,包括订单编码,时间 戳或时间属性,区块链的长度,区块链的分支数,地理位置或空间属性,买家确认情况,卖家确 认情况,算力值和占比,并计算所选择的所有属性的最优裁决方案;进一步地,裁决方案的评估 是多目标的,裁决的优化目标可以考虑区块链的分叉最少,或单根区块链的长度最长,交易时间 间隔最小,算力约束小于51%;

[0041] 子步骤3-3c:计算最近两次裁决优化结果的精度误差有没有小于ε_1,或进行裁决优化是否达 到最大次数限制;如果误差符合精度要求或达到最大次数限制,则进行下一个子步骤,输出裁决 结果;如果误差不符合精度要求或未达到最大次数限制,则返回到前一子步骤,继续优化裁决结 果;

[0042] 子步骤3-4,裁决结果输出;得到最优的冲突裁决结果后,可以由多个冲突裁决智能体通过 区块链网络将冲突裁决结果发送到裁决后执行智能体;

[0043] 子步骤3-4a:根据群体智能算法输出的最优裁决向量的位置,判断冲突匹配值大小,对交易 冲突裁决结果按匹配值高低进行排序,以便于后续的冲突执行按照优化的冲突匹配值从高到低处 理;进一步地,可以根据用户需求对冲突裁决结果按交易优先级排序,以便于后续的冲突执行按 照优先级从高到低处理;

[0044] 子步骤3-4b:进一步地,把最优交易冲突向量的位置、与之相应的冲突匹配值、属性匹配值、排序结果输出;

[0045] 所述的方法,其特征在于,所述步骤4,裁决执行,包括以下步骤:

[0046] 子步骤4-1,接受裁决结果;多个裁决后执行智能体接收冲突裁决智能体发送来的裁决结果, 包括对应的智能合约、冲突匹配值、属性匹配值;

[0047] 子步骤4-2,智能合约智能体执行;对应的智能合约执行裁决结果,由多个裁决后执行智能 体通过区块链网络控制智能合约智能体的执行;进一步地,不同的裁决优化结果有不同的执行结 果;优选地,对于形成区块链新分叉的智能合约交易,自动放弃分叉记账,而将本次交易区块链 接到最长的区块链上;优选地,对于两次复制同一笔交易的冲突,智能合约自动取消后一笔交易; 优选地,对于用户确认状态不正常的交易,智能合约自动取消该笔交易;优选地,对于算力超过 51%的智能合约交易,可以取消该笔交易;

[0048] 子步骤4-3,数据区块智能体执行;多个裁决后执行智能体通过区块链网络控制数据区块智 能体的执行,所有区块完成共识后进行分布式记账,本次交易和智能合约的执行将无法抵赖;进 一步地,检查本次区块链分支的数量,并比较分支的长度,将较短分支上的区块连接到长分支区 块链上,以便维护整个区块链为一根无分支的、较长的区块链;

[0049] 子步骤4-4,执行结果返回;返回本次记账结果,以及区块链的长度;进一步地,本次交易 结果和分布式记账可为下次冲突裁决提供匹配依据。

[0050] 一种基于群体智能的区块链智能合约的冲突裁决系统,它包括多个智能合约智能体、区块链 网络、多个数据区块智能体、多个冲突匹配智能体、多个冲突裁决智能体、以及多个裁决后执行 智能体;多个智能合约智能体与区块链网络双向连接,多个数据区块智能体与区块链网络双向连 接,多个冲突匹配智能体与区块链网络双向连接,多个冲突裁决智能体与区块链网络双向连接, 多个裁决后执行智能体与区块链网络双向连接。

[0051] 与现有技术相比,本发明具有如下技术效果:

[0052] 首先,本技术方案能够快速地匹配智能合约冲突,并实现智能裁决。本发明针对现有技术的 不足而设计的一种基于群体智能的区块链智能合约的冲突裁决方法,采用粒子群-遗传混合算法, 根据不同属性差异进行匹配计算和裁决优化。多个智能合约智能体,多个数据区块智能体,多个 冲突匹配智能体,多个冲突裁决智能体,多个裁决后执行智能体,通过区块链网络协同工作,使 得分布在不同区域的智能体可以高效快速地判断出智能合约交易是否会发生冲突况,并根据用户 需要和冲突优先级,进行裁决的智能优化,使用最优的裁决方案来解决交易冲突问题。

[0053] 其次,本技术方案能够有效避免区块链分叉冲突。区块链分叉是本技术方案中冲突匹配的重 要属性,群体智能协同判断交叉冲突提高了交易阶段在分叉判断时的效率。尤其在冲突匹配和执 行冲突裁决的过程中,均应用了分叉判断计算,在快速匹配分叉冲突的同时,也保留了记账的高 效性。群体智能协同匹配分叉冲突问题,有效解决了多交易方在运行区块链智能合约时无法判断 是否会产生新分叉的问题。

[0054] 再次,本技术方案能够有效避免分布式数据的一致性问题和冲突问题。群体智能通过匹配时 间戳和位置信息,能够快速判断交易冲突和数据不一致问题。裁决的智能优化方案还可以根据用 户需求和冲突优先级协同解决冲突,多个智能合约智能体与多个数据区块智能体协同工作,大大 降低了区块链智能合约交易中产生不一致数据的可能性,提高了数据冲突匹配和冲突裁决的效率。无论多个交易方还是攻击者的短时间重复数据操作都会产生不一致的时间戳,从而被群体智能发 现,从而禁止了对共享数据的修改。攻击者也无法知晓本次攻击是被个智能体所匹配而发现的。 智能裁决和智能执行能够有效维护数据一致的状态,攻击节点不能简单地并发执行智能合约交易。

[0055] 最后,本技术方案能够抵御多种攻击导致的冲突问题。本技术方案可将用户确认

状态、时间 戳和算力列入冲突匹配属性。因此，在本技术方案中，多个智能体能迅速发现比特币转账交易等 操作中是否存在冲突。即使对于更复杂多变的交易条件和攻击环境，多个智能体协同工作也能准 确匹配出智能合约交易多方之间的交易属性是否发生冲突。群体智能为了保证交易的正常进行和 冲突智能裁决，会不断迭代计算，即使攻击者持续攻击，也无法影响区块链的正常工作和智能合 约的正常运行。

附图说明

[0056] 下面结合附图和实施例对本发明作进一步说明：

[0057] 图1为本发明中系统的结构框图；

[0058] 图2为本发明的工作流程图。

具体实施方式

[0059] 如图1所示，一种基于群体智能的区块链智能合约的冲突裁决系统，它包括多个智能合约智 能体101、区块链网络102、多个数据区块智能体103、多个冲突匹配智能体104、多个冲突裁决 智能体105、以及多个裁决后执行智能体106；多个智能合约智能体101与区块链网络102双向 连接，多个数据区块智能体103与区块链网络102双向连接，多个冲突匹配智能体104与区块链 网络102双向连接，多个冲突裁决智能体105与区块链网络102双向连接，多个裁决后执行智能 体106与区块链网络102双向连接。

[0060] 智能合约智能体101，优选地，为客户端计算机或客户端手机，并在客户端计算机或手机上 安装具有一定智能的区块链智能合约交易软件。智能合约软件具有分布式多节点管理层，负责智 能合约的编写和触发、提供智能合约接口，向用户提供安全、透明的数字版本。智能合约智能体 101必须能够运行用户要求的所有智能合约交易协议，兼容用户交易所需的各类智能合约协议， 且其运行完全无需人工干预，具有一定的智能，能够自动执行任务和交易，甚至可以根据存储在 其代码中的规则来限制交易行为。智能合约交易参与者通过智能合约智能体101分别用各自私钥 进行签名，以确保合约的有效性。智能合约智能体101确保每个交易者访问区块链数据库只能看 到自己的交易记录和与自己有关的数据，以确保智能合约的保密性交易。

[0061] 进一步地，智能合约智能体101，可分为客户端和服务器端，提供客户登录注册界面，交易 更新界面，交易条件确定界面等；优选地，用于公网查询的智能合约智能体101，可以采用局域 内部网Intranet或因特网Internet Web服务器，系统网络结构包括在中心局域网以及广域网。相关硬件参数：Web服务器CPU型号选用Intel Xeon Silver 4210，CPU频率2.2GHz，CPU十核， 20线程，主板芯片组Intel C622，内存类型DDR4，内存容量16G，32G，64G，128G，硬盘接口SATA。本实施例中客户服务端是最主要的输入输出介质，使客户与计算机进行交互，用于把原始数据和 处理这些数的程序输入到计算机中。计算机接收数值型或非数值型的数据，如图形、图像、声音 等，通过不同类型的输入设备输入到计算机中，进行存储、处理和输出。磁盘运用INSPUR八通 道高性能SAS RAID卡RS0820P(2G缓存)，Web/COM+服务器磁盘，Web/COM+服务器可进行IIS 5.0Web服务和COM+服务，并且通过配置群集提高系统性能的扩展性，客户服务端接收计算机数 据的输出显示、打印、声音、控制外围设备操作等，也是把各种计算结果数据或信息以数字、字 符、图像、声音等形式表现出来。网

络控制器选用INSPUR八通道高性能SAS RAID卡RS0820P(2G 缓存)。输入设备主要包括:键盘,鼠标,摄像头,扫描仪,光笔,手写输入板,语音输入装置 (麦克风)等。常见的输出设备有显示器、打印机、绘图仪、影像输出系统、语音输出系统、磁 记录设备等。

[0062] 进一步地,智能合约智能体101,该智能合约模板中是存在与区块链中,由其他用户通过智 能合约语言(Solidity、Serpent、LLL编程语言)进行编写,通过如以太虚拟机进行运行,通过不 同的校验节点,进行确认后而部署在区块链上的。当以上必要变量由A用户和B用户填写完整后, 会由算法程序会提取必要变量,然后进行转化后智能合约语言,如将以上信息转化为Solidity 编程语言,然后匹配到已经选择的智能合约模板中,生成一份属于A用户和B用户之间的专属的 完整的区块链智能合约。区块链智能合约采用DHT分布式哈希表的网络储存方式,智能合约会通 过ICE协议的P2P方式在区块链智能合约网络中广播一个包含合约集合Hash值的区块结构,其 他验证节点发送一份本验证节点认可的合约集合,以区块结构形式发送最新达成的合约集合到全 网。

[0063] 区块链网络102,优选地,为各类有线或无线网络设备,能够同时连接多个智能合约智能体 101,多个数据区块智能体103,多个冲突匹配智能体104,多个冲突裁决智能体105,多个裁决 后执行智能体106。

[0064] 数据区块智能体103,是区块链中的节点,用于存储智能合约交易数据,优选地,使用具有 存储功能的计算机或手机,并安装具有一定智能的区块链智能合约存储软件。区块链智能合约通 过网络协议以P2P方式在区块链网络102中广播交易信息,每个区块链节点都会收到一份合约交 易数据。数据区块智能体103必须能够运行用户要求的所有智能合约存储协议,且其运行完全无 需人工干预,具有一定的智能,将会自动接收广播的合约交易数据,收到之后自动保存到本地节 点的存储单元中,与其他数据区块智能体103共同完成共识。数据区块智能体103在降低签订合 约、执行和监管方面的成本的同时,也提高了合约验证和执行过程的速度。

[0065] 进一步地,数据区块智能体103,使用集成的存储单元,如果以软件功能单元的形式实现并 作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。本发明实现上述实施 例方法中的全部或部分流程,也可以通过计算机程序和指令实现的硬件来完成,所述的智能合约 计算机程序可存储于计算机可读存储介质中,该计算机程序在被处理器执行时,可实现上述各个 方法实施例的步骤。其中,所述计算机程序包括计算机程序代码,所述计算机程序代码可以为源 代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质可以包括:能够 携带所述计算机程序代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机 存储器、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、电载波信号、电信信号以及软件分发介质等。所述计算机可读介质包含的内容可以根据司法管辖 区内立法和专利实践的要求进行适当的增减,例如在某些司法管辖区,根据立法和专利实践,计 算机可读介质不包括电载波信号和电信信号。

[0066] 进一步地,数据区块智能体103,存储了智能合约数据,交易冲突裁决结果,及冲突匹配和 裁决过程涉及的所有数据,包括交易方的信息,交易记录,交易条件,冲突条件,并对各方数据 进行分块存储和加密存储,确保数据的保密性。多个数据区块智能体103构成分布式账本,能够 在无人工干预情形下进行自主管理,并对交易中的各种数据进行分块存

储,分为公有区域和私有 区域。数据区块智能体103的公有区域包括所有发生在区块链网络交易中的产生条件,交易请求, 冲突条件,交易记录和判断记录,私有区域含有用户自身的交易数据和记录。优选地,数据区块 智能体103的数据库开发环境使用ModelArts的MoXing,构建于TensorFlow、PyTorch、MXNet、 MindSpore等深度学习引擎之上,提供简单易用的分布式计算框架MoXing API/SDK,使得这些计 算引擎在分布式冲突匹配和冲突裁决时获得更高性能;而用于交易条件与记录的数据库可选择 ACCESS数据库和/或Cassandra数据库;以上区块链智能合约的分块数据存储库可采用区块链分 布式数据库和GIS数据库。数据区块智能体103的区块是一串使用密码学方法相关联产生的数据 块,每一个数据块中包含了一批次智能合约交易的信息,用于验证其信息的有效性(防伪)和生 成下一个区块存储于其中的数据或信息,具有去中心化、公开透明、独立安全、集体维护等特征。

[0067] a.数据区块智能体103去中心化;通过分布式的核算和存储,各个数据区块智能体103实现 了信息自我验证、传递和管理,所有数据区块智能体103节点能够在系统内自动安全地验证、交 换数据,不需要任何人为的干预;

[0068] b.数据区块智能体103公开透明;除了交易各方的私有信息被加密外,数据区块智能体103 的数据对所有人开放,任何人都可以通过公开的接口查询数据区块智能体103数据和开发相关应 用;

[0069] c.数据区块智能体103独立安全;只要不能掌控全部数据节点的51%,数据区块智能体103 就无法肆意操控修改网络数据,这使区块链本身变得相对安全,避免了主观人为的数据变更;

[0070] d.数据区块智能体103集体维护;除非有法律规范要求,单从技术上来讲,数据区块智能体 103各区块节点的身份信息不需要公开或验证,信息传递可以匿名进行,整个过程要靠多个数据 区块智能体103一起来维护。

[0071] 冲突匹配智能体104,优选地,使用高性能计算机或手机,并在计算机或手机上安装具有一 定智能的区块链智能合约冲突匹配软件。进一步地,也可根据某种选举算法,在智能合约智能体 101中选举一定数量节点作为冲突匹配智能体104。参与交易冲突匹配的冲突匹配智能体104必 须先注册成为区块链智能合约的合法用户,区块链返回给用户一对公钥和私钥。冲突匹配智能体 104必须能够运行用户要求的所有智能合约的冲突匹配算法,兼容用户交易所需的各类智能合约 协议,且其运行完全无需人工干预,具有一定的智能,使用公钥做为用户在区块链上的账户地址, 私钥做为操作该账户的唯一钥匙。两个及以上的用户确定首次交易条件后,即共同商定一份承诺 合约进行冲突匹配,并对整个冲突匹配过程进行安全和隐私保护。当多方的交易数据进入区块链 网络102,冲突匹配智能体104会自动将其归入拥有智能合约类型码的条件数据集中,统计某些 类型条件与其他不相匹配且不成比例的出现频率,由冲突匹配算法判断交易是否冲突条件,根据 匹配值的大小捕捉数据集间的相异之处。若条件相匹配,则冲突匹配智能体104判定为交易不冲 突,直接将交易信息反馈给区块链网络102,继续交易。

[0072] 冲突裁决智能体105,优选地,使用高性能计算机或手机,并在计算机或手机上安装具有一 定智能的区块链智能合约冲突裁决软件。进一步地,也可根据某种选举算法,在智能合约智能体 101中选举一定数量节点作为冲突裁决智能体105。冲突裁决智能体105必须能够运行用户要求 的所有智能合约的冲突裁决算法,兼容用户交易所需的各类智能合

约协议,且其运行完全无需人 工干预,具有一定的智能,合约中包含了双方的权利和义务。冲突裁决智能体105所规定的裁决 权利和义务以电子化的方式设计记录下来,并反馈到数据区块智能体103。冲突匹配智能体104 判定智能合约交易不匹配,即冲突发生,则冲突裁决智能体105自行判定发生冲突的原因,由冲 突裁决优化算法挖掘最优的冲突裁决结果,并制订合理的策略,阻断不合法的交易过程或攻击过 程,放弃不合法的记账数据,将冲突对区块链的损失和影响降低到最小。冲突裁决智能体105通 过区块链网络102将裁决结果反馈到裁决后执行智能体106,并指导多个智能合约智能体101和 多个数据区块智能体103执行优化后的裁决结果。

[0073] 裁决后执行智能体106,优选地,使用高性能计算机或手机,并在计算机或手机上安装具有 一定智能的区块链智能合约冲突后执行软件。进一步地,也可根据某种选举算法,在智能合约智 能体101中选举一定数量节点作为裁决后执行智能体106。裁决后执行智能体106必须能够运行 用户要求的所有智能合约的冲突裁决算法,兼容用户交易所需的各类智能合约协议,且其运行完 全无需人工干预,具有一定的智能,能够通过区块链网络102接收冲突裁决智能体105发送的裁 决执行结果,并控制智能合约智能体101和数据区块智能体103准确执行裁决结果。

[0074] 图2为本发明一实施例提供的一种工作流程图,它包括以下步骤:

[0075] 步骤1,裁决初始化;区块链智能合约会定期检查自动机状态,逐条遍历每个合约内包含的 状态机、事务以及触发条件;将条件满足的事务推送到待验证的队列中,等待共识;未满足触发 条件的事务将继续存放在区块链上。进入最新一轮验证的事务,会扩散到每一个验证节点,与普 通区块链交易或事务一样,验证节点首先进行签名验证,确保事务的有效性;验证通过的事务会 进入待共识集合,等大多数验证节点达成共识后,事务会成功执行并通知用户。主要子步骤包括:

[0076] 子步骤1-1,设置冲突裁决参数;可以为常见的智能合约冲突设置匹配和裁决参数,常见的 冲突包括区块链分叉的冲突,分布式数据的一致性问题和冲突问题,多种攻击导致的冲突问题, 例如比特币竞态攻击,双重支付攻击和芬尼攻击,51%算力攻击等导致的冲突问题。优选地,对 应的冲突匹配属性和裁决参数可以选择,区块链分叉数量,区块链长度,时间戳,区块地理位置, 用户交易的确认状态,数据一致性,用户的算力等。

[0077] 子步骤1-2,采集智能合约参数;区块链智能合约采用DHT分布式哈希表的网络存储方式, 共识时间到来之后,验证节点会把该时间区间内收到的所有合约打包成一个合约集合Assemblage; 并计算该集合Assemblage的Hash值;将合约集合Hash值封装在一个区块里,然后广播该智能 合约交易信息。收到合约集的节点,都会对每条合约进行验证,验证通过的合约才回最终写入区 块链中,验证的内容主要是合约参与者的私钥签名是否与账户匹配且交易方的私钥只能访问属于 自己的地址和数据库区域。

[0078] 子步骤1-3,采集交易消息;所有验证节点采集智能合约的交易信息,会分解出该结构里合 约集合Hash值,与本验证节点Hash集合下的Hash值做比较;再发送一份本验证节点认可的合 约集合给其他节点,通过这种多轮的发送和比较;所有的验证节点最终在规定的时间内对最新的 合约集合达成一致。最新达成的合约集合会以区块的形式扩散到全网。

[0079] 子步骤1-4,信息发送;每个区块可发送的信息包括:当前区块的Hash值、前一区块的Hash 值、达成共识时的时间戳、以及其它描述信息;另外,区块链最重要的信息是带有一

组已经达成 共识的合约集。

[0080] 步骤2,冲突匹配;优选地,使用粒子群-遗传混合算法作为冲突匹配核心算法。当多个交易 冲突同时发生时,多个冲突匹配智能体104能够自行运行粒子群-遗传混合算法,匹配是否发生 冲突,判断交易冲突的优先级,分析智能合约交易中冲突的发生原因。主要子步骤包括:

[0081] 子步骤2-1,智能体接收消息;

[0082] 子步骤2-2,冲突匹配;群体智能算法中的粒子群算法针对大自然里粒子群的回声定位搜索 目标进行了模拟,运用粒子群的搜索性能来寻找空间个体,可在复杂区块链环境中对冲突目标进 行搜索,智能优化群体行动中的局部解,以解决冲突匹配问题。该算法具有模型简单,参数配置 少,收敛速度快等优点,可应用于在智能合约冲突属性匹配、冲突裁决多目标优化等问题中。

[0083] 子步骤2-3,属性匹配值计算;为了避免基本粒子群算法陷入局部最优分析问题中,本技术 文件采用遗传算法对粒子群算法进行了优化改进,构成了粒子群-遗传混合算法,来进行多交易 冲突中冲突属性匹配和冲突裁决最优解的搜索。

[0084] 子步骤2-4,匹配值输出;

[0085] 步骤3,冲突裁决;在本技术方案中,采用遗传算法产生的最好子代与基本粒子群算法产生 的子代进行再竞争的方法,让算法在后期依然能够具备丰富的种群多样性,结合遗传算法中的选 择、交叉、变异机制能够丰富种群多样性,避免局部最优问题发生,提高后期收敛速度。主要子 步骤包括:

[0086] 子步骤3-1,冲突匹配值输入;

[0087] 子步骤3-2,群体智能裁决计算;将区块链智能合约交易中的多个冲突进行粒子群算法的运 算,在进行遗传算法操作时,将当前粒子群种群及适应度值作为遗传算法的初始种群和初始适应 度值,初始种群按照适应度,分别进行选择、交叉、变异,以形成子代。

[0088] 子步骤3-3,群体智能优化裁决结果;通过离差的方法选取与全局最优值差异最小的子代和 基本粒子群算法的随机生成子代,分别计算适应度值并比较,适应度值小的子代作为粒子群局部 搜索的备选粒子群,从而优化冲突裁决的目标函数。让粒子群-遗传算法的种群模拟自然界中自 然选择的方法产生后代,得到更加适应环境的最优后代,即找到冲突裁决问题的全局最优解。基 于粒子群-遗传算法的冲突裁决算法赋予区块链以智能,使其可自行感知区块链智能合约中发生 的交易冲突,并根据用户需要优先处理某一交易中的冲突,同时将最优的冲突结果反馈给区块链 执行。

[0089] 子步骤3-4,裁决结果输出;

[0090] 步骤4,裁决执行;冲突裁决完成后,智能合约会自动执行裁决结果,其自带的状态机会判 断所属合约的执行状态,当合约包括的所有冲突裁决事务都顺序执行完后,状态机会将合约的状 态标记为执行完成,并从最新的区块中移除该合约;反之将标记为执行进行中,继续保存在最新 的区块中等待下一轮执行处理,直到冲突裁决全部处理完毕;主要子步骤包括:

[0091] 子步骤4-1,接受裁决结果;

[0092] 子步骤4-2,智能合约智能体执行;整个裁决结果执行事务和执行状态的处理都由区块链底 层内置的智能合约智能体系统自动完成,全程透明、不可攥改,且智能合约的数

据无法删除、修 改，只能新增。连接到网络的每个智能合约智能体设备都有一份合约副本，并且数据会永远保存 在网络上。智能合约因为链上的资源是真实透明的，合约的内容确定后就无法更改，执行更是不 用依赖任何额外操作。合约缔结前，智能合约智能体无需进行信用调查，缔结后也不用第三方进 行担保履行，从而大大降低交易成本，大幅提高执行效率。

[0093] 子步骤4-3，数据区块智能体执行；智能合约根据逻辑来编写和运作，只要满足输入要求， 也就是说只要代码编写的要求被满足，合约中的义务将在数据区块智能体中便可得到执行。数据 区块智能体执行裁决结果时效率更高，不可逆转，是安全的交易以及全自动化流程。在执行裁决 结果时，涉及到的交易条件是否产生新的冲突，由数据区块智能体分布式运行和同时判断，并执 行最优的裁决结果。数据区块智能体能够记录冲突裁决执行结果并返还客户端，判断冲突裁决执 行效果及剩余冲突情况，在最短时间内达到最优的冲突裁决效果。数据区块智能体执通过结点连 接的散状网络分层结构，能够在整个网络中实现信息的全面传递，并能够检验信息的准确程度。这种特性一定程度上提高了区块链智能合约交易的便利性和智能化。数据区块智能体执具有十分 自由的进出能力，可独立的参与或离开区块链体系，不对整个区块链体系有任何干扰。

[0094] 子步骤4-4，执行结果返回。冲突裁决执行结果的记账由分布在不同地方的多个节点共同完 成，而且每一个节点记录的是完整的账目，因此它们都可以参与监督交易合法性，同时也可以共 同为其作证。本技术方案中区块链每个节点都按照块链式结构存储完整的数据，而非传统分布式 存储中将数据按照一定的规则分成多份进行存储。本技术方案中区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，而非传统分布式存储中通过中心节点往其他备份 节点同步数据。本技术方案中没有任何一个节点可以单独记录账本数据，从而避免了单一记账人 被控制或者被贿赂而记假账的可能性。随着记账节点的增多，本技术方案出现冲突的可能性越来 越低，除非所有的节点被破坏，否则账目就不会丢失，大提高了账目数据的安全性。

[0095] 在本发明一实施例中，假设存在甲，乙，丙，丁四个用户，包括以下冲突裁决步骤。

[0096] 步骤1，裁决初始化；主要子步骤包括：

[0097] 子步骤1-1，设置冲突裁决参数；

[0098] 子步骤1-2，采集智能合约参数；多个智能合约智能体101采集智能合约参数，甲乙丙丁分 别注册签订智能合约，在交易双方签名完智能合约之后，将广播该智能合约到区块链网络中，交 易各方首次出交易条件。

[0099] 子步骤1-3，采集交易消息；多个智能合约智能体101采集交易消息，甲提出a,b,c三个交 易条件，乙提出a一个交易条件，丙提出b,c两个交易条件，丁提出a,b,c三个交易条件。

[0100] 子步骤1-4，信息发送；当甲和乙，甲和丁，甲和丙，甲乙和丙同时提出交易请求后，可能 发生冲突，信息通过区块链网络102发送出去。

[0101] 步骤2，冲突匹配；主要子步骤包括：

[0102] 子步骤2-1，智能体接收消息；

[0103] 子步骤2-2，冲突匹配；多个冲突匹配智能体104运行所述的基于粒子群-遗传的冲突匹配算 法，进行交易条件差异挖掘，发现甲丙交易条件匹配，直接将甲丁交易条件反馈

给区块链网络102，判定为交易不冲突，继续交易。甲乙，甲丙，乙丙条件不匹配，判定为交易冲突。

[0104] 子步骤2-3，属性匹配值计算；多个冲突匹配智能体104确定条件不匹配即冲突后，则计算 属性匹配值，分析冲突的原因，并根据属性匹配值挖掘有差异的冲突交易条件，甲乙冲突交易条 件为bc，甲丙冲突交易条件为a，甲乙丙冲突交易条件为abc，反馈到多个冲突匹配智能体104，将 冲突条件通过区块链网络102存入多个数据区块智能体103。

[0105] 子步骤2-4，匹配值输出；

[0106] 步骤3，冲突裁决；主要子步骤包括：

[0107] 子步骤3-1，冲突匹配值输入；

[0108] 子步骤3-2，群体智能裁决计算；多个冲突裁决智能体105运行粒子群-遗传混合算法，来进 行多交易冲突中冲突优先级和冲突最优解的求解，采用遗传算法产生的最好子代与基本粒子群算 法产生的子代进行再竞争的方法，结合遗传算法中的选择、交叉、变异机制，通过算法得出优先 级从高到低为甲丙冲突，甲乙冲突，甲乙丙冲突，并判断执行优先处理甲丙交易中产生的冲突， 再将冲突条件返还给多个智能合约智能体101，同时冲突数据和最优解记录反馈给多个数据区块 智能体103。

[0109] 子步骤3-3，群体智能优化裁决结果；多个冲突裁决智能体105据优先级处理，甲丙冲突条 件为a，甲乙冲突条件为bc，甲乙丙冲突条件为abc让交易方甲乙丙在客户服务端观察并判断是 否继续进行交易，甲丙，和甲乙选择继续交易，甲乙丙三方冲突条件不在交易方的接受范围内， 则交易终止。

[0110] 子步骤3-4，裁决结果输出；多个冲突裁决智能体105运行粒子群-遗传混合算法优化裁决结 果，甲丙，和甲丁选择继续交易，则客户服务端将选择交易终止的交易方甲乙丙提出的交易条件 在本次交易中排除，然后继续交易的各方提出新的交易条件，甲丙交易中，甲提出bc，丙提出bc， 甲乙交易中，甲提出ab，乙提出a，交易条件和数据存入数据库。进入区块链智能合约网络并再 次判断是否冲突，甲丙交易条件不冲突，则交易各方继续进行交易。甲乙交易条件仍然冲突，将 冲突条件重复返还给客户服务模块，循环步骤3-1，3-2，3-3。直至冲突裁决优化结束后，输出冲 突裁决优化结果。

[0111] 步骤4，裁决执行；主要子步骤包括：

[0112] 子步骤4-1，接受裁决结果；在实例中，多个裁决后执行智能体106接收甲乙丙丁分别交易 是否发生冲突的情况以及优化的冲突裁决结果，并判断冲突优先级，按优先级从高到低处理冲突， 也可按用户需求定义顺序进行，执行冲突裁决结果直至交易全部顺利完成。

[0113] 子步骤4-2，智能合约智能体执行；多个裁决后执行智能体106控制多个智能合约智能体101 执行智能合约，直至甲乙两个交易方顺利进行交易，不再发生交易冲突的情况或者甲乙有一方交 易方选择继续进行交易，交易直接终止。

[0114] 子步骤4-3，数据区块智能体执行；多个裁决后执行智能体106控制多个数据区块智能体103 记录所有交易记录，交易条件，冲突条件等信息。数据区块智能体103分为公有区域和私有区域， 公有区域包括所有发生在区块链网络交易中的产生条件，交易请求，冲突条件，交易记录和判断 记录，私有区域含有用户自身的交易数据和记录。

[0115] 子步骤4-4，执行结果返回。智能合约智能体101和数据区块智能体103通过区块链

网络102 向裁决后执行智能体106返回执行结果。

[0116] 本技术方案实施例运用了基于群体智能的粒子群-遗传混合算法,使用区块链智能合约自动 匹配交易冲突,优化冲突裁决,自动执行裁决结果,解决了现有技术区块链智能合约交易存在交 易冲突和攻击的问题。

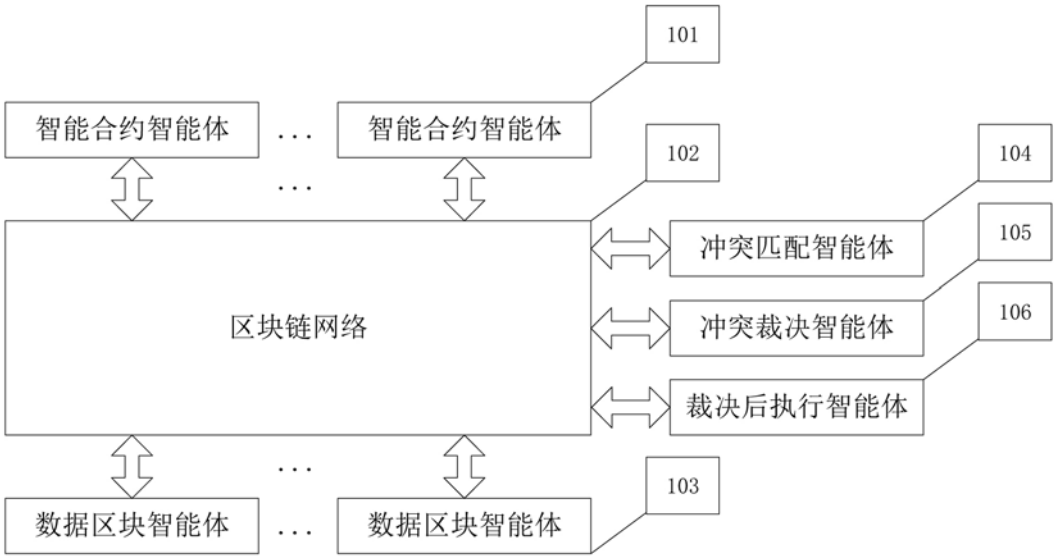

101
智能合约智能体
智能合约智能体
102
104
105
106
区块链网络
冲突匹配智能体
冲突裁决智能体
裁决后执行智能体
103
数据区块智能体
数据区块智能体

图1

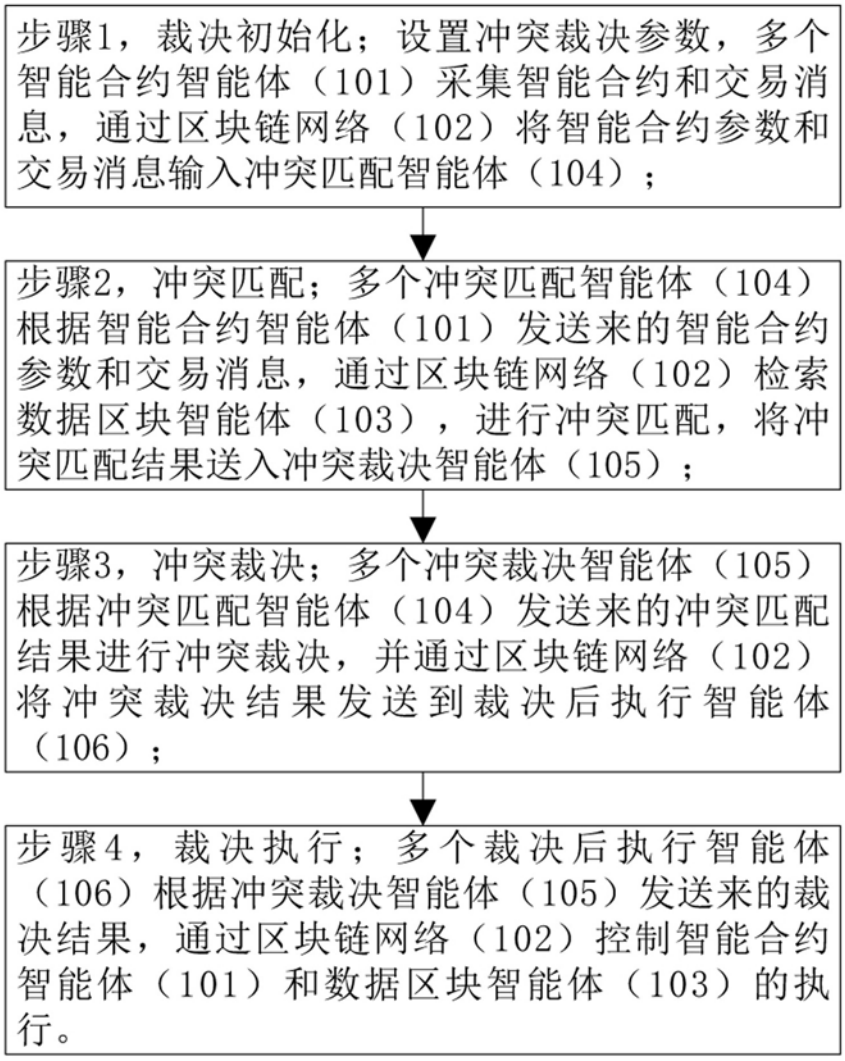

步骤1，裁决初始化；设置冲突裁决参数，多个智能合约智能体（101）采集智能合约和交易消息，通过区块链网络（102）将智能合约参数和交易消息输入冲突匹配智能体（104）；
步骤2，冲突匹配；多个冲突匹配智能体（104）根据智能合约智能体（101）发送来的智能合约参数和交易消息，通过区块链网络（102）检索数据区块智能体（103），进行冲突匹配，将冲突匹配结果送入冲突裁决智能体（105）；
步骤3，冲突裁决；多个冲突裁决智能体（105）根据冲突匹配智能体（104）发送来的冲突匹配结果进行冲突裁决，并通过区块链网络（102）将冲突裁决结果发送到裁决后执行智能体（106）；
步骤4，裁决执行；多个裁决后执行智能体（106）根据冲突裁决智能体（105）发送来的裁决结果，通过区块链网络（102）控制智能合约智能体（101）和数据区块智能体（103）的执行。

图2